Great Treasure of Hengqin: The New Mount Sinai

横琴大秘宝：新贵的西奈山

与 AI 全球监控斗争的考试场

软弱了的美国科技公司与美国政府合作，正计划使用针对电子产品的 US Cyber Trust Mark 法规、Matter 区块链、Ambient 标准、AI digital twins 等等监管手段建立无孔不入的新世界秩序。如果不现在开始旗帜鲜明的对其迎头痛击，海外华人、世界无产阶级人民将丧失自由的火种。

目录



一， 澳门的新元横琴

1594 年，葡萄牙传教士在澳门创办了远东地区的第一所大学。横琴作为澳门多元化的延申。在传承历史的基础上，针对当前时代最紧迫的 AI 科技对隐私的威胁，横琴可以成为服务世界无产阶级人民与 AI 科技假神斗争的培训中心和演练场。

1.1， 横琴的 LPWAN 频谱优势

《中华人民共和国工业和信息化部公告 2019 年第 52 号》 ：“微功率短距离无线电发射设备”“无需取得无线电频率使用许可、无线电台执照、无线电发



射设备型号核准”。 对应的附件文档:《微功率短距离无线电发射设备目录和技术要求》 对 470Mhz-510Mhz 要求是“发射功率谱密度限值: 占用带宽小于等于 200kHz 的，为 50mW/200kHz(e.r.p)”。

中国大陆基于 470Mhz-510Mhz 的 LoRaWAN 低功耗广域物联网网络已经在多个城市部署且应用于多个行业。广州技象科技有限公司成立于 2018 年，是中国电子科技集团公司（中国电科）科技成果转化和混合所有制改革的科技企业。其业务是“聚焦物联网底层关键技术，打造 100%自主知识产权的 TPUNB 物联专网，推进窄带无线通信技术的行业标准和国家标准体系建设。”中国电科是中央直接管理的国有重要骨干企业，在国内军工电子和网信领域占据技术主导地位。

2019 年，美国商务部将中国电科及其多个子公司列入了实体清单（Entity List）。美国政府指责中国电科及其相关公司参与了与中国政府的军事和安全项目，特别是涉及到军事现代化、电子战和通信技术等敏感领域，因此将其纳入黑名单。

目前，中兴通讯、腾讯、阿里巴巴、中国联通、铁塔公司、贵州广电等加入了 LoRa 物联网领域，2018 年中国市场 LoRa 芯片出货量占全球一半以上。

很显然，在中国大陆，470Mhz-510Mhz 频段是会长期免授权使用的，并且可以合法用于建立低功耗无线广域物联网网络（LPWAN）。横琴在没有官宣归属澳门管辖之前，遵守中国大陆法规，故此，在横琴部署 LPWAN 低功耗无线广域物联网网络是合法的。



澳门法律明文禁止非官方运营的无线网络覆盖。根据《第 198/2014 号行政长官批示》“用于公众服务的无线区域网络（Wireless LAN）仪器，必须通过电信管理局所作出的认可程序。且公众服务范围只规限于室内或指定地点，不得跨越公共道路或公共地方，同时亦不可以此建立一个覆盖全澳门的公共电信网络。”

但是澳门法规许可符合美国标准的免授权无线频谱频段 920-925 MHz，且最大许可功率达 1 W，与美国标准相同。

依照中国大陆法律，920Mhz 频段是不能免授权使用的。但是澳门大学在横琴驻地适用澳门法律，920Mhz 频段是可以免授权使用的。而且信号覆盖范围穿越横琴地区的道路是在横琴明确归属澳门管辖之前澳门法律无法管辖的。某研究院匿名消息人士称，澳门大学计划扩建，在横琴中心地区成立新校区，从 8000 人扩展到 2.5 万人的规模。

中美科技对抗中，物联网系统是一个关键领域，它涉及到数据安全，AI 数字孪生的数据源头，中国能否实现独立自主的科技愿景，以及人民群众的平安。当前，美国政府与马斯克代表的科技资本深度合作，不断扩展法规，许可新的频率，建立新的标准，提高能量上限，打开捆龙锁，意欲在众多未来愿景的实现上与中国公司拉开距离，保持领先。众多中国本土科技公司试图与之抗衡，但受限于频谱法规：东南亚、中东等新兴市场与美国或欧洲的频谱法规相

同，920Mhz 频段免授权使用，而中国大陆对 470-510Mhz 免授权，这使得中国大陆的公司在实验和公开展示用于出口到美国标准地区的大规模物联网系统时无真实建筑物可用。如果在海外建立样板工程作为展示场地，不仅增加了成本，而且增大了研发机密泄露的风险。特别是在应对人形机器人自杀炸弹式恐怖袭击，自爆无人机攻击等需要实时做出反应的智能建筑安防应急无线网络系统中，需要类似军事演习场的真实 5A 级建筑物作为样板实验。

在上述背景下，将横琴打造成一个中美免授权频率都可使用的地区，从而能建立真实的实验测试场景，让美国科技公司的最新物联网系统在这里充分得到部署和实验，以便促使中国科技公司进行对照。对中国科技公司构成一个真实的考试比武场，可以在不泄露自身研发机密的前提下，对自身产品提前做出应急反恐能力评估和改进升级。对国家投资基金，中东主权基金投资人，国际游资投资者提供可见的反恐、应急、低碳等效果展示，相当于科技时代的比武融资擂台。

1.2，横琴的互联网直连优势

某熟知澳门政策的匿名消息人士称：2025 年，横琴地区即可直接使用 YouTube 等美国公司提供的网络服务，与澳门等同。这一优势使中国科技工作者与美国隐私保护科技组织进行合作成为可能，共同对抗 AI 与物联网系统对人民隐私的潜在威胁。



可在横琴引入的对抗 AI 监控的美国隐私保护科技社团组织:

（1），Tor 网络（The Onion Router） 是一个旨在保护用户在线隐私和匿名性的开放源代码网络系统。它通过“洋葱路由”技术，将用户的互联网流量多次加密，并随机传输到多个中继节点，使通信难以追踪。Tor 网络可以匿名浏览网站、发送信息以及访问暗网。最早的比特币发展基于暗网，而暗网基于 Tor 网络，所以可以说，Tor 网络是 BTC 之母。

Tor 的早期开发资金部分来自美国海军研究实验室（NRL），DARPA（美国国防高级研究计划局）。现在资金来源包括：NGO 电子前哨基金会（EFF），Mozilla 基金会，Reporters Without Borders（无国界记者组织），美国国务院的民主、人权和劳工局（U.S. Department of State Bureau of Democracy, Human Rights, and Labor），志愿者捐赠。技术支持包括麻省理工学院（MIT），剑桥大学、斯坦福大学等。

2024 年 10 月 17 日，Silvia Puglisi 和 Roger Dingledine 代表 Tor 网络在 DEFCONConference 上发言:

“Cryptocurrency world, their fundamental building block is capitalism, is maximizing profit. And the Tor World, our fundamental building block is altruism, it's I want to make the world a better place, I have extra resources I can provide them. So these are very different worlds.”

“加密货币世界的基本组成部分是资本主义，正在实现利润最大化。而 Tor 世界，我们的基本组成部分是利他主义，我想让世界变得更美好，我有额外的资源可以提供给他们。所以这是非常不同的世界。”



（2）Zcash：Zcash 是一种注重隐私和安全的加密货币，于 2016 年推出。它基于比特币协议，但引入了零知识证明技术（zk-SNARKs），允许用户在交易中隐藏发送方、接收方和金额等信息，从而提供更高的隐私保护。同时，Zcash 还支持透明交易，用户可自行选择隐私级别。

爱德华·斯诺登：“我以笔名约翰·多伯丁参加了 Zcash 原创仪式”。

截至 2024 年 12 月，香港证券及期货事务监察委员会（证监会）已向七家虚拟资产交易平台（VATP）颁发牌照，允许其在香港合法运营。自 2021 年 9 月起，中国全面禁止了加密货币的挖矿活动。加密货币交易在香港已经合法化。目前在澳门，加密货币挖矿的合法性没有明确的官方禁止性规定，因此与大陆不同，澳门并没有完全禁止挖矿活动。横琴互联网如 2025 年与澳门相同直连国际互联网，则运行 Zcash 服务器并与 Zcash 组织合作研发并测试隐私保护的匿名加密货币成为可能。

（3）P2P 加密通讯软件 Keybase：《中华人民共和国网络安全法》（2017 年）要求网络运营者对用户数据进行保护，同时规定政府部门有权在必要时获取数据。这与端到端加密的核心理念（即数据仅对通信双方可见）产生一定冲突。所以国内几乎没有 P2P 加密的通讯软件。而海外华人、我国驻外大使馆、世界无产阶级人民在 AI 流量监控，MetaData 分析的威胁下，需要不记录手机号，不记录 MetaData 的 P2P 加密通讯软件，而且需要防止网络



IP 追踪系统。澳门无相关禁令。横琴处于中间地带，正是引入匿名服务器，和欧美多个 P2P 加密 IM 合作的最佳地点。

1.3，横琴的影响力优势

横琴已经拥有大量 5A 级高层建筑物，而当前入住率不高，这些建筑物的维护需要投入巨大资金。而 LPWAN 正适合用于建筑维持，且本文提到的用于隐私保护，对抗 AI 监控的 Mesh 无线网络，部署在建筑物后，可以形成一个天然的测试场。将维护资金变成建设资金，教育资金，在不增加支出的前提下，完成了人才培养、产品出海测试的任务。

在横琴建设初期，各个国企央企都竞相在此地兴建高层建筑，保利集团等都有建筑物在此，只要相关项目成功，可以获得较大影响力，从而快速向相关公司的海外项目推广。

二，美国将用 AI 监管世界

美国是世界上最大的经济体，也是全球军事基地最多的国家。以川普 2024 年的再次当选为标志，美国国内矛盾必然会向全球传导。以马斯克为代表的科技资本，提供了监管全球的科技工具：AI、星链。结合加强安全认证的物联网协议，一场打着科技进步的幌子，实则打造科技监控囚笼的全球新秩序战争开始了。

2.1，芯片自然科学发展到顶

现代城市运行在芯片和代码之上。摩尔定律（Moore's Law）是由英特尔公司联合创始人戈登·摩尔（Gordon Moore）于 1965 年提出的一项预测，其核心内容是：在价格不变的情况下，集成电路上可容纳的晶体管数量每隔约 18-24 个月就会翻一番，计算性能也会随之指数级增长。摩尔定律是基于自然科学作为锚定的，它表明了人们可以使用更低的成本获得更高的算力，用更低的价格买到同等功能的电子产品。

但是，人类在自然科学神坛上的增长在 7nm 后遇到了瓶颈。7nm 之后，芯片制造中的边际收益下降，工艺节点的推进在成本、性能和能效上的改进增量已经趋于减少，而研发和生产的复杂性和成本却显著增加。

晶体管尺寸进入纳米级别后，电子在极小的栅极间隙中更容易穿越，导致漏电增加。晶体管密度增加使散热变得更困难，影响芯片的可靠性和效率。先进工艺节点需要极紫外光刻（EUV）技术，其设备极其昂贵。更小的节点需要更复杂的电路设计，EDA 工具成本和开发时间显著增加。制程缩小使得生产中缺陷率上升，增加了流片的失败风险。晶体管数量的增加并未完全转化为显著的性能提升，单核性能增长趋缓。电压降低和功耗减少空间有限，能效改善变得越来越困难。

在 3nm 和 2nm 节点，单位晶体管的制造成本比 7nm 高出 30%-50%。从 10nm 到 7nm，性能提升约为 20%-30%，但从 7nm 到 5nm 及以下，性能改进趋于 10%-15%。流片周期显著延长，设计失败的风险更高，进一步增加边际



投入。

- 7nm 节点：单次流片成本约为 2000 万美元。
- 5nm 节点：单次流片成本增加至约 3,000 万美元。
- 3nm 及更先进节点：流片成本突破 5,000 万美元，且良品率进一步成为成本压力。

由于高流片成本，只有顶尖企业（如苹果、英伟达、AMD）能够承担，行业门槛大幅提高。初创公司和中小企业逐渐转向成熟节点（如 28nm 或 14nm）开发高性价比产品。相当于行业发展到顶，停滞。

戈登·厄尔·摩尔（Gordon Earle Moore）于 2023 年 3 月 24 日在夏威夷的家中逝世，同时，Intel 公司也走衰。

不论从物理知识上，还是代表人物、代表公司的表现上，都可以说明芯片发展在自然科学上已经无以为继，无法维持过去 40 年的高速增长。

2.2，芯片公司大并购

台积电（TSMC）的 7nm 工艺技术首次推出于 2018 年，同时，芯片行业正在进行剧烈的并购，很多伴随着芯片科技一同出现的活化石公司名字消失。

2015 年，NXP 约 115 亿美金收购飞思卡尔；2016 年 10 月，高通约 400 亿美金打算收购 NXP，后未经中国反垄断审批而失败；2015 年，微芯科技（Microchip）约 32.5 亿美金收购 Atmel；2016 年，安森美（ON Semiconductor）约 29 亿美金收购仙童（Fairchild Semiconductor）；2020 年，英伟达（Nvdia）



计划 400 亿美元收购 ARM，因未通过反垄断批准未遂；2020 年，AMD 约 350 亿美元收购赛灵思（Xilinx）；2020 年，Analog Devices (ADI) 约 210 亿美元收购 Maxim Integrated (美信)；2021 年，瑞萨电子约 60 亿美元收购 Dialog Semiconductor；2018 年，瑞萨电子约 67 亿美元收购了 IDT（Integrated Device Technology）；2019 年，英飞凌约 90 亿美元收购赛普拉斯（Cypress Semiconductor）；2018 年，微芯科技约 83.5 亿美元收购美高森美（Microsemi）。

推动芯片行业在自然科技层面不断进步的一个又一个公司被收购，标志着行业进入了下行。

2.3，AI：人文假神的崛起

芯片科技在自然科学方面发展到顶，表现在经济活动上就是，中国不断获得成熟制程技术，而美国 Intel 等公司停滞不前，无法继续创新。在这一背景下，美国的生态发生了巨大变化，政治上表现为高举美国优先政策的川普上台，经济上表现为以 AI、人形机器人、星链等脱离了自然科学发展方向的人文科技假神的崛起。

（1）AI 与创新无关，只与算力和数据有关，换句话说，只与资本和政策有关：获得一个 AI 模型，只需要三个要素：输入的数据，要得到的输出数据，训练用的算力。算力消耗资本，在欧美法制下，数据也要付费。AI 开发变成了烧钱比赛。

2023 年 1 月，微软投资 OpenAI 公司约 100 亿美元，2024 年 9 月，不



到两年时间，这笔钱就将耗尽。

AI 模型训练对于资本的要求，使得爱迪生式的发明家无法在这一领域发生。而另一方面，有了足够的资本和数据，AI 模型就能被训练出来。这一事实说明，AI 模型训练领域并不是类似传统自然科学的创新者公平赛道，而更多的是资本的造神场。

（2）**AI 假神领导，使用者跟随：** 一个领域一旦被 AI 攻克，完成某项工作，你只需要按照 AI 的提示一步一步执行。职业技能的差异被消除了，随之而来的只有一个权威：AI。个人在职业技能上的投入在 AI 时代变得多余，此时，AI 变成了工作场所的领导权威，工作人员变成了 AI 的棋子。

一旦一个应用可以使用 AI 模型解决，那么意味着这一领域不再需要具有自主性的工作人员，资本家不再依赖高智慧的科技工作者来维持其体系运行。大量的程序员被 AI 取代就是一个直接的表现，随着机器人技术的发展，这一取代也会发展到建筑工人等体力依赖的行业，进而对各行各业产生摧枯拉朽的冲击。

（3）**AI 决策更多是人文逻辑:**

AI 不依赖于人力，必然导致比传统资本主义更严重的供应过量，迫使美国科技公司秩序向全球扩张，补充消费者。

又因为 AI 可以被恐怖分子利用，所以 AI 服务的门槛一定是某种世界通用的信用积分，类似信用评级一样的系统。如果被 AI 认为信用分值低，就只提供非常基础的 AI 服务，如果被 AI 认为信用分值高，就提供非常完备的 AI 服务。

给人评级打分，本身就是一个人文科学，不是自然科学。从这个角度上讲，



AI 出现后，竞争已经不是自然科学上的竞争，而变成了人文科学的假神竞争。使用哪个 AI 大模型，就是使用者感觉哪个 AI 大模型对他的判断更加公平。但是我们的经验和知识告诉我们，世上没有理想国，当 AI 假神倒塌的时候，造成的灾难一定是更加巨大的!

2.4，物联网标准协议：AI 的车同轨书同文

在 AI 兴起的同时, 连接标准联盟 CSA（Connectivity Standards Alliance）也开始活跃，推动物联网协议的统一标准，为 AI 监控帝国铺平道路。

2021 年 5 月，Zigbee Alliance 宣布更名为 Connectivity Standards Alliance，并将发展重点转向新的智能家居互联标准 Matter。看似只是简单的改名，实则是能量等级跳跃式提高，发展方向由向上探索变为向下限制。

寡人早在 2008 年就参与了使用 Zigbee 协议部署的山东省济南市省科技厅办公楼智能建筑节能项目。当时 Zigbee 自组网技术学术讨论较多，项目案例更多是一种前端探索和实践测试。在实际的控制系统测试中，因为自组网的多跳增加了延时，加上当时 MCU 处理器速度普遍较慢（8Mhz，8bit MCU），所以有比较明显的延时，直观感受不佳。Zigbee 标准的智能家居产品也一直未在全球市场占据一半以上的主导地位，故影响力尚未成型。

2021 年全球遭遇疫情期间，逆势成立的连接标准联盟 CSA，整合了内置 IPv6 的 Thread 开源无线自组网协议、蓝牙 BLE 协议、WiFi 协议等，主导了 Matter 标准的开发。Matter 协议的目标是为智能家居设备提供统一、开放且安全的连接标准。CSA 联盟的最高会员（Promoter）包括：Apple（苹果公司）、



Google（谷歌公司）、Amazon（亚马逊公司）、Samsung（三星公司）、NXP Semiconductors（恩智浦公司）、Qualcomm（高通公司）、Signify (原飞利浦照明)、Ikea（宜家）、Harman、Legrand、Lutron、Resideo、Broadcom（博通公司）、Vizio、Chamberlain Group、Eaton、Zebra Technologies、LG Electronics。可以说缔结了欧美公司最精锐力量。CSA 推动 Matter 协议，致力于推动设备之间的互操作性和标准化。其愿景是让消费者能够轻松地选择和连接不同品牌、不同平台的智能家居设备，确保设备的安全性和长期可用性。

CSA 的 Matter 标准正在举着为消费者服务的旗帜一统江湖，但是很显然的，一统江湖之后将引入 AI 进行监管。IPv6 的引入使得 AI 大模型可以使用现有针对计算机的软件不加修改就可以运用到更深入生活的各种电子设备上，真正做到无死角监控的全球超级天网系统。

可以说，推行 Matter 标准是一次物联网领域的美国科技公司巨头们对中小公司的“消藩”操作。一旦“车同轨，书同文”，所有电子产品将无缝迎来 AI 接管。美国科技公司背后的资本就可以通过 AI 与物联网系统监控世界。

三，举起隐私保护教育的大旗

在这一历史洪流下，我们爱好自由的人们，应当坚定的举起隐私保护教育的大旗，在美国法制生态和语境下，为世界人民的自由斗争。无产阶级只有解放全人类才能最后解放自己。

3.1，中国无法孤立于世界

中国政府文官对待欧美强大的科技力量进入中国，在过去 40 年改革开放的历史上普遍采取了如下几种策略:

1, 使用基础物理指标制定有别与欧美的中国标准，达到与欧美产品技术标准区分的效果，从而限制欧美技术标准产品的直接大举进入中国市场，保护了自己的运作空间。比如说美国标准规定免授权频谱是 920Mhz，而中国标准规定免授权频谱是 470Mhz，这就使得美国市场上销售的无线通讯产品无法直接拿到中国市场销售。

2, 扶持国内同类科技公司发展，对欧美技术逆向工程，从而缓和欧美技术产品在中国占领主流市场。比如说，扶持中国国产手机品牌以应对苹果手机。

3, 签订市场换技术条款，或者通过谈判要求外资投资工厂等拉动就业，对欧美技术力量进行捆绑，从而为己所用。比如说富士康工厂，如果离了工人，工厂也无法正常运转，所以文官政府与富士康管理层形成了一种制约。

在美国科技发展调头向下，由自然科学增长转向人文假神增长的历史洪流下，文官政府原有的这些策略将统统失效。

1, 美国的 Matter 等标准在国际通用免授权频段 2.4Ghz 上运行，又通过种种技术扩大了它的通讯距离。使用物理参数进行限制的方法无法对已经大量部署的 WiFi、蓝牙等进行管制，进而这种限制无效化。



2, 扶植国内同类公司发展的前提条件是，中美公司的基础发展平台，或者说赛道的底层是自然科学，两者是在公平的平台上进行竞争，这样国内公司还有可能获取一席之地。而人文假神化的科技标准，本身的底层是人文的协议，类似某种政治口号的表态。比如 CSA 的 Matter 标准，本身规定了底层协议和应用，这种情况下，扶持进入 Matter 协议的国内公司就等于给 Matter 标准送弹药。那能否构建一个类似 Matter 的物联网标准呢，当然能，但是欧美公司不承认，泾渭分明，这样就没有达到在同一个概念下浑水摸鱼的效果。比如说手机概念下有苹果手机和国产某某手机，苹果手机和某某手机都是手机，都有屏幕，甚至操作界面还可能差不多，这样消费者在选择的时候就可能选择国产的某某手机。而 Matter 标准产品突出 Matter 这个人为标准，它就是一个根概念，这个根概念下挂载各种日常电子产品，消费者认准了 Matter 认证购买之下的音响和灯泡，消费者认为 Matter 这个概念和国产的某某标准是两个完全不同的东西，如同两个不同的政党一样，泾渭分明，所以国产的某某标准无法达到任何抵抗效果，还可能起到反衬作用。

3, 过去高速发展的 40 年，是人民群众生活水平从低到高，从无到有，从俭入奢的过程。现在人民群众城市生活被欧美科技产品所捆绑，如果没有欧美的芯片等外来科技输入，中国的城市生活水平下降，所以市场换技术，试图使用工人捆绑美国的人文科技发展方向的科技公司，这已经是本末倒置。



在这种情况下，国家大力投资半导体行业，试图内循环。内循环的本质是降低要求，但是在不完全关闭国门的情况下，只要国内科技产品与欧美科技产品有落差，有钱有能力的人民还是会向往欧美产品，所以形成了人群分类和筛选，进而形成了新的阶级。可以说，越孤立，越内循环，用过好东西的人民群众越向往欧美产品, 越有强大的动力打破孤立主义屏障, 所以, 中国孤立主义是个死胡同。

另外, 中国共产主义是国际主义, 国际主义必然肩负着解放全球人民的责任, 所以搞孤立主义是背信弃义, 必然遭到世界无产阶级人民的唾弃, 从这个角度上, 中国也不能搞孤立主义。

3.2，在美国法制语境下旗帜显明的斗争

既然孤立主义走不通，主动融入历史洪流是必然之选。如何在美国法制环境下进行有效的斗争，是这一节主要说明的问题。美国法制是一个能量瓶颈高的万神殿机制, 做假神引得全球人民敬拜是合法的, 如同马斯克的星链项目做的那样。同样隐私保护这一对抗 AI 监控的领域也是合法的，此时，旗帜鲜明的举起对抗 AI 监控的隐私保护大旗是最有利的。

在电动车、AI 人形机器人、星链等新技术出现后，世界人民的隐私面临的威胁达到了前所未有的历史高度。你可以用手机打开电动车的车门，意味着电动车和你的手机账户是绑定的, 手机账户又一般是注册在某个美国巨头互联网公司的，而电动车又安装了 GPS 定位系统、四周摄像头，并且，电动车一般是联网的。这样，你是谁，你在何时何地打开了车门，甚至是此时车的周边环境如何,



都有可能被黑客恐怖分子群体获取，进而威胁你的安全。一旦电动车电子系统被入侵，车内的摄像头可以暴漏你的影像，车内声控系统麦克风可以暴漏你的声音，这是在燃油车时代前所未有的。AI 人形机器人当被黑客入侵后可以认为是一个行走的间谍，它有眼可以看，有耳可以听，并且可以通过互联网将情报随时传到世界任何一个角落。对于带有 AI 功能的电脑而言，你可以通过粘贴摄像头阻挡贴等物理遮挡方式确保一些隐私保护措施的有效，而对于 AI 人形机器人而言，你很难物理上阻挡一台被黑客控制的机器人获取信息。星链的部署使得太空图像加 AI 分析变得廉价，进而使得山顶别墅等传统的隐私保护方式失效。不论大小贫富，世界人民都面临着隐私泄露的考验。人们必然慢慢觉醒认识到这一点，所以此时旗帜鲜明的举起隐私保护的大旗，并对世界人民进行宣讲是应景的。

已经有不少欧美公司在从事隐私保护的业务，但是多是针对传统领域，而未有对 AI 技术的威胁做出应对。比如：瑞士公司 protonmail 针对邮件进行加密。此时，重点聚焦于对抗 AI 技术，可以填补市场空白，并且与现有的隐私保护组织进行合作。

3.3，利用横琴特区缓冲内外落差

出于维稳考虑，国内技术能量天花板与国际技术能量天花板存在落差，隐私保护技术在欧美环境是合法的，但是在中国大陆却是受到各种法规限制的。苹果公司可以拒绝 FBI 的解锁恐怖分子苹果手机的要求，而按照中国国安法等法规要求，有关部门可以向任何组织和个人要求提供协助，所以国内任何一家手机公司都必须配合解锁用户手机，如果政府有关部门要求的话。这也是中国大陆公司



的隐私保护产品难以在世界兴盛的重要原因。

中美对抗成为主要矛盾后，中国驻外大使馆人员，中国海外情报人员等群体隐私保护、身份隐匿技术要求陡然提高，而 AI 技术的应用使得监控系统空前强大。一方面是海外华人的迫切隐私保护需求，一方面是国内文官政府的维稳法规，两者冲突的中间地带一直是香港，但是香港很显然在当前时间段内不被北京信任，而又在被美国作为攻击的标的。此时，横琴作为一个近乎无人的处女地，非常适合承担缓冲国内外能量落差，作为出国华人的隐私保护训练场所使用。

3.4，使用教育名义风险下放

隐私保护在国内政府维稳官员的视角解读就是“杀人放火查不出来”，而欧美公司提供的多是付费后就可以使用的软件或者硬件，这种方式姑且不考虑付费记录是否会被查到的问题，在文官政府看起来，这无异于“出售杀人执照”。而因为出售产品后，产品可以在世界任何地点使用，所以出现问题后还是会追查到产品供应方组织，最终有可能被“远洋捕捞”，所以欧美公司的直接出售商品的隐私保护产业模式在中国走不通。

任何技术都可以用于行善或者作恶，能调整的只有让使用者获得这种技术的门槛，是花费金钱获得，还是通过某种考试认证获得。欧美体制下，公司或者个人拥有的财富一般是和其自律程度成正比的，所以欧美公司可以使用金钱作为技术能量等级提供的门槛，即只要付钱，就可以提供最高等级的隐私保护技术，如果使用者用于犯罪，那是整个社会信用评估系统的问题，而不是这个公司的问题。但是很显然，这种逻辑在中国是失效的，2024 年中国公开判刑的亿元上贪官至



少有 37 个。使用金钱作为隐私保护技术扩散的门槛在中国是必然会出问题的，所以不能模仿欧美公司的模式。

使用教育培训的方式，将个人技能作为门槛，提供的硬件软件是欧美体制下合法的已经存在的且多用途的，必须通过一定的编程，整合后才能达到隐私保护，抵抗 AI 监控的效果。这么做使得任何国家的政府都无法直接追查到横琴，因为技能、思想是在人脑中的，也没有标签，少数能力掌握者犯罪，也不能怪罪到培训组织上来。比如任何学校都不能保证培养的学生日后不会变成恐怖分子，即使学生日后变成恐怖分子了，也无法怪罪到学校上来。但是如果把学校换成军火供应商，学生变成军火买家，那么军火买家犯了罪，就有可能牵连到军火供应商。所以，使用隐私保护教育的名义将风险隔离，风险下放，是必须的和长治久安的必然之举。

四，银弹：Mesh 网络零碳建筑应用

对比美国科技公司拉帮结伙缔结全球优秀人力物力，我国处于相对弱势，无法全面对抗，在这种情况下，只能选择像当年原子弹计划一样，集中精锐人员，选择几个重点方向进行突破。设想在不久的未来，包括智能家居在内的民用领域也被 AI 和 Matter 物联网标准占领，智能音箱等可以随时监听使用者谈话的严酷背景下，我们用什么技术可以有效的保护人民的隐私?

这种技术体系要求:

- 成本低，每个无产阶级人民都可以消费的起
- 有很大操作空间，可以用于很多应用所以 AI 无法彻底摸清



- 可以较远距离通讯防止被定位
- 可以加入随机量，从而让 AI 难以摸清内部逻辑，达到隐私保护效果
- 在欧美合法，已经有大规模的部署案例，不会被行政命令撤销
- 可以应用于多种商业，生产，生活等应用，不与隐私保护直接相关，有巨大的商业前景
- 每个应用都有巨大的使用量，难以被追踪和管控，可以以商业公司名义扩散这一技术

综上考虑，寡人经过长时间寻找摸索，最终得出结论：可编程的 Mesh 网络节点既是这种技术。

4.1，Mesh 网络正在国际市场获得成功

总部位于芬兰坦佩雷（Tampere）的物联网公司 Wirepas 的无线 Mesh 节点已经部署了一千万个。其中 400 万个是 2024 年在印度部署的，使用了美国公司 Silicon Labs 的芯片。因为美国公司大量吸收了欧洲优秀公司的技术，这些上了美国科技公司全球化标准扩张这趟列车的欧洲公司的产品会被这股力量推动而快速大量部署。

Wirepas 公司的核心技术是 Wirepas Mesh，一种用于物联网设备的去中心化、可扩展、高效的无线网络协议。具有以下特点:

- 完全分布式：没有中心控制节点，所有设备均可动态决定网络拓扑。
- 高可扩展性：网络可以支持从数十个到数百万个设备的无缝扩展。
- 低功耗：通过优化通信机制，设备可在电池供电模式下运行多年。



- 频谱高效：支持多信道通信，减少网络冲突并提高传输效率。
- 硬件无关性：兼容多种无线芯片和平台，包括蓝牙低功耗（BLE）、Sub-GHz 频段等。
- 灵活性：支持点对点（P2P）、多跳（multi-hop）和广播等通信模式，适应不同应用场景。

主要应用领域：

- 工业物联网：包括工厂自动化、设备监控、数据采集等。
- 智慧城市：智能路灯、交通信号控制、环境监测等。
- 智能楼宇：建筑能源管理、智能传感器网络。
- 资产跟踪：物流行业中物品的实时定位和状态监测。
- 智能电网：用于能源计量和电力设备管理。

Wirepas 公司只提供 Mesh 网络算法，其底层芯片来自合作伙伴，包括：

- Nordic Semiconductor：代表欧洲的无线芯片。
- Silicon Labs：代表美国国家队的无线芯片。
- Qorvo：美国军工射频领域服务商。

以下是 2024 年 7 月的新闻稿：Wirepas and the Silicon Labs' EFR32FG23 Sub-GHz SoC are taking on India's Smart Metering Challenge:

"在 2021 年，印度宣布了一项现代化电网的计划，旨在减少损耗并提高运营和财务效率。该计划的一个重要部分是引入智能电表并建设印度的高级计



量基础设施（AMI）。截至 2023 年，Silicon Labs（芯科科技）和 Wirepas 在印度智能电表市场取得了初步成功，其成功的关键在于结合使用 Wirepas 的 Sub-GHz LPWAN 解决方案和 EFR32FG23 (FG23) Sub-GHz SoC。Silicon Labs 和 Wirepas 的整体解决方案目前占到该计划部署的 700 万只智能电表中的约 100 万只，随着 AMI 计划的持续推进，到 2024 年预计将迎来大幅增长。

印度政府计划完成智能电网项目的规模和时间表，给这一新兴市场带来了前所未有的挑战。Wirepas 和 Silicon Labs 通过提供一种不依赖任何集中式基础设施（如基站、路由器或集中器）的连接解决方案，来应对这些挑战。每个智能电表都配备了一块运行 Wirepas 连接软件的网络接口卡（NIC）。由于 Wirepas 去中心化网状网络架构的特性，以及 FG23 的内存占用小和高度集成的优势，这种组合成为这些应用的理想选择，能够降低 NIC 设计的成本和复杂性。

基于 FG23 的 NIC 使用标准协议（如 DLMS）与电表通信，用于读取电表指数和发送配置指令。同时，NIC 通过完全自动化和去中心化的多跳网状网络连接到网关，每个电表都可以作为其他电表的路由器。网关随后将数据转发到头端系统（HES）或电表数据管理（MDM）系统，供公用事业公司访问和分析数据。

AMI 推广过程中，市政当局面临的最大挑战之一是如何安装和配置这些新建网络。传统上，这些网络需要由专家团队设计并针对每个具体环境进行优化，但使用 Wirepas 的情况下并非如此。Wirepas 网络从安装第一块电表起



就开始形成，并随着每块新增电表上线而自动扩展，对安装电表的电工几乎无需额外操作。

FG23 的顶级射频性能消除了对昂贵且复杂的网络规划或额外网络基础设施的需求。凭借超过一英里的点对点通信范围，FG23 能够连接到最偏远的电表，实现网络的监控和控制。然而，大多数智能电表将部署在节点密集的城市区域。在这种情况下，Wirepas 协议使 FG23 能够通过找到未被占用的信道以最低所需功率进行通信，而不会影响网络的其他部分。

这种架构在免许可的 865 MHz 频谱中具有显著优势，与许可的蜂窝频谱相比，能够在小范围内连接更多节点。

最后，这些网络的正常运行时间和安全性对于印度实现其项目目标至关重要。严格的服务水平协议（SLA）被应用于这些新兴网络，以确保基础设施所有者能够及时对每个电表采取行动。Wirepas 网络的特性使其能够通过灵活性和无单点故障的设计实现极高的正常运行时间。随着电表的添加或移除，网络能够快速适应并保持通信，几乎没有延迟，也不会中断连接。这种能力使 Wirepas 和 FG23 能够满足印度市场独特的严格响应时间要求。根据规定，90%发送到电表的指令必须在初始请求后 15 分钟内成功完成。由于电表分布广泛，使用蜂窝技术实现这一要求存在挑战，但通过 Silicon Labs 和 Wirepas 的解决方案却轻松实现了这一目标。

Wirepas 和 FG23 的解决方案为印度 AMI 市场带来了变革性影响，提供了一种可扩展、可靠且安全的连接方案，以满足智能电网项目的挑战和需求。与基于蜂窝的解决方案相比，该解决方案能够显著降低实施和运行成本。



它充分利用了 Wirepas 和 Silicon Labs 各自在 LPWAN 和无线 SoC 技术领域的优势。在印度市场已经部署了 100 万只智能电表，并将在未来部署更多。Wirepas 和 Silicon Labs 联手，有潜力改变印度电力行业的格局，为更加高效和可持续的能源未来铺平道路。”

2024 年 11 月，根据新闻稿，此项目已经有 400 万个装载有 wirepas 自组网协议的表被部署。随着这种城市级百万个节点的项目被验证，Mesh 网络技术已经经过案例检测，并且在美国国家队科技公司的强力资金助推下，可以预见的，Mesh 网络技术在新兴的东南亚，中东等市场会迎来井喷式增长。

4.2，将横琴建筑维护费变 Mesh 教育投资

横琴地区的兴建是在中国经济高速增长期，现已经建成了大量的 5A 高档写字楼，工程接近完工就遇到疫情，而后房地产增长失速，2024 年中国经济增长在贸易战等外部因素下，增长放缓。5A 级建筑物维持运转需要消耗大量资金，横琴作为新区，人口较少，新兴产业尚在起步阶段。可以预见的，在相当长一段时间内，横琴的建筑物维护费是一个只花钱不挣钱的无底洞，而且这个费用还是一个可观的数字。在这种情况下，需要为这些建筑物的维护费找到一个合理的使用意义，或者转变为投资，Mesh 网络教育正是这样一个项目。在 5A 建筑物内部署 Mesh 无线网络，接管建筑物的灯光、制冷、安防、门禁水表、电表等系统，如果不计算人工费用，只计算硬件费用，花费很小。问题是，凭什么有个人或者组织愿意来一个没人的 5A 建筑物以不盈利的目的部署这些 Mesh 无线节点呢？答案是：Mesh 网络技术在国际市场正在增长期，类



似当年学会数理化走遍天下都不怕一样，掌握了这门技术相当于拥有了进入国际市场的专家证，这是从个人职业发展的角度考虑。另一方面，我国驻外大使馆，驻外情报人员，海外华人，任何有一定资产想要隐匿的人，在 AI 大发展的时代，对于隐私保护是一个刚需，而这种需求又很难花钱解决，所以出于自身隐私保护的考虑，也会有大量的教育培训需求。那么教育培训最好是需要一个真实的场景，一个真实的模拟欧美城市的地区，这个地区人口密度低，监控系统使用最先进的 AI，物联网系统使用最新美国标准的，这样可以很好的观测哪些信息可以被 AI 分析得到。这么考虑，横琴就是一个最合适的地点。一方面是大量的建筑物维护费用只有投入没有意义，另一方面是海外华人，我国驻外大使馆，情报人员，出国富商强烈的适应 AI 监控时代隐私保护的教育训练需求，两者的结合之处就是使用横琴的 5A 级建筑物部署 Mesh 物联网网络加 AI 监控系统提供隐私保护培训。

4.3，私有 Mesh 网络吃掉部分互联网平台市场

一旦建筑物的私有 Mesh 网络建立完成，下一步必然会秩序被动扩张到部分互联网平台应用。因为 Mesh 网络去中心化的特征，所以前期会以超低的成本向外扩张。建筑物附近 1 公里的物联网小系统，甚至是短消息服务，都可能免费。

在我国电信网络部署初期，存在单位部署的“小灵通”电信私网，手机号使用短号码，只要在这个区域内的就可以免费通话。现在这种 5G 私网在美国也是合法部署的，但是在中国因为种种原因，被禁止了。但是在物联网领域，一方面是只有会编程的人才可以动用这个网络，即存在一定技术门槛，第二是我国驻外



人员面临美国 AI 监控的威胁，必须发展私网技术以对抗监控，在这种历史背景下，城市级部署的私网 Mesh 物联网就有可能迎来大发展。

一旦 Mesh 网络部署，就可以用于支付系统等，达到隐匿手机持有者地理位置的效果。这样带有隐私保护功能的城市级 Mesh 网络就有潜力极大的分走属于传统互联网平台公司的信众，从而具有巨大的市场盈利前景。

综上，不论是从隐私保护安全的角度考虑，还是从发展扩张的角度考虑，城市级私有 Mesh 物联网网络部署一旦完成，都有巨大的长久的获利。在中美对抗的大背景下，中国的能量天花板会进一步抬高，这正是历史机遇。

4.4，相控阵列定向通讯加 Mesh 扛无线侦测 AI

我们再来看 Mesh 网络本身能否对抗 AI 的监控。欧美的 Mesh 网络研发方向侧重于性能，即部署后通电就可以使用，同时清晰的提供路由表，拓扑结构。但是我们的 Mesh 设计突出于隐私保护，所以我们必须对欧洲的 Mesh 网络技术进行一定的改动。我们假定最恶劣的情况，中国驻美国大使馆部署一套 Mesh 网络，美国间谍人员可以使用最先进的频谱和协议分析仪器来监控空域。试问，何种 Mesh 算法最能保证安保系统正常工作?

第一，混入相控阵列定向通讯的节点。这些节点可以与几个固定的节点使用相控阵列天线进行定向通讯，这样通讯的信道就不容易被嗅探，从而进行一层保密。

第二，混入只收不发的暗节点。暗节点把信息通过相控阵列定向通讯传递到其它节点。暗节点因为本身只收不发，所以很难被空口仪器探测到。



第三，发送数据中混入随机数和延时量。确保 AI 无法分析出数据协议、控制命令等核心参数。

在这些领域，又需要大量的实战测试，大量的新技术，新专利，而横琴提供了这样的一个测试场，可以容纳世界顶尖公司前来测试、展示、演练、比武，进而推向全球隐私保护市场。

4.5，建筑物 Mesh 可以扩展到反无人机等军火级对抗系统

我们再来关注军事系统。Mesh 网络最开始的研发就包括了军事系统应用，包括智能弹药，无人蜂群，战地情报检测等。俄乌战争爆发后，战场形态极大的被无人机和 AI 系统改变了。传统坦克等越大的目标，越容易被 AI 识别并被 AI 无人机自动攻击，大量 AI 控制的无人载具的使用，使得现代战争更重于隐藏自身，保密。可以说，只要知道目标人物在建筑物的哪个房间，特工人员就可以向弹簧刀、金牛座等 AI 控制的无人机下达命令实时外科手术式的打击，整个过程无需人为干预，即使失败也只是消耗一架无人机，而不会暴漏特工人员的位置和身份等信息。在这种情况下，隐私保护就是和自身的性命息息相关。而，AI 加 mesh 网络在抵御网络刺探的基础上，还可以对偷拍等刺探情报的无人机进行风险评估，隐私泄露评估，甚至是使用高能激光武器攻击，或者是出动防御无人机进行防御等措施。

目前的建筑物，控制系统都是中心式的，别说防御入侵的无人机了，自己的



系统中心一旦被攻击就立即瘫痪，而 mesh 网络无中心，一个节点坏掉，网络立即自愈合组成新的网络，不会瘫痪整个系统。可以说，mesh 网络是在未来高保密建筑物防无人机刺探的必然之选。而在横琴可以部署和向全球演示这些系统，从而向全球人民提供平安。

五，执行计划

5.1，在横琴部署 470Mhz LPWAN 抢占频谱

这是最简单最快速且成本极低，潜在收益巨大的首发行动。只要使用公司名义与具有地点的个人或者组织签订意向合同就可。寡人已经选择了全球可以通用的不受中美贸易战科技战影响的中国台湾芯片厂提供的无线芯片，并完成了初步评估测试。只要将无线节点作为公司资产装载入某个横琴的公司，并且与拥有放置地点的第三方签署公开的公益 LPWAN 运营合同，运行这个节点，就可以认为横琴地区已经部署了 470Mhz 无线通讯网络，构成了既成事实。这样不论澳门法律如何修改，必须兼容已经存在的系统。如果澳门法律不允许跨路系统，则此系统成为独有的系统，构成了垄断，将获取更大利润!

一旦拥有意向合同，就可以进一步融资，扩大声势与影响力。



5.2，与学校合作推进欧标 868Mhz，美标 920Mhz 无线节点

虽然澳门法律许可 920Mhz 美标，但是横琴并未实施澳门法系。但是大学校区除外，比如说澳门大学校区虽然在横琴，但是实行澳门法律，那么很显然，教育用的无线节点可以使用 920Mhz，这样就可以和大学合作，以教育项目的名义实施美标 920Mhz 的 Mesh 网络项目。

868Mhz 需在此观点得到一定规模认可后（有案例项目，有全国各地年轻人参与，有全球公司关注，有中东资金投资等等），政府正式承认横琴的频谱特区地位，然后申请得到许可。这一计划可以放在第二步。

5.3，小规模部署：别墅级 Mesh 网络案例

建筑物大小类似我国驻德国柏林大使馆，类似一栋别墅。别墅的水电控制，节能控制，附近的停车，安防，都使用 Mesh 网络进行。并且记录过程，作为教育案例使用。

同时引入全国 AI 公司，使用无线干扰电战设备，进行评估测试。比如说，使用无人机加载电战设备，进行干扰，看安保系统是否依然正常工作。

测试得到的经验数据和技术算法，申请专利，并发表相关论文。



5.4，楼宇部署：高层建筑维护 Mesh 网络案例

在别墅级小规模部署得到经验的基础上，开始部署楼宇项目。构建楼宇内部独立的网络系统，防止入侵、无人机干扰刺探的影响，同时有较高的智能化，能够提前发现建筑物隐患。降低维护费，同时使用 AI 模拟，将建筑物向零碳改造方向提供网络支撑和数据支撑。争取建成第一个低人流，高舒适度，零碳，低维护费，高度隐私保护的 5A 级高层建筑物，并使用国际认可的区块链记录建筑物内数据获得国际公信力。

5.5，城市部署：横琴一张私有 mesh 网，满足传统互联网业务

支付支持，本地电商支持，房屋租赁业务，外卖业务，租车业务，导航业务，目前所有全球互联网提供的服务，都可以在城市私有 mesh 网络上实现，但是同时包含了对使用者的隐私保护功能。

拥有这一 Mesh 网络的公司将拥有长久的声誉和全球知名度。

六，结尾的话

很多年之后，人们回忆这段经历时会说:

Sons and daughters of Chinese sacrificed their lives to “defend a land they never knew and a people they never met.”



中华儿女倾倒自己的生命，去“解放一个他们从未了解的土地（AI 监控下的世界）和一个他们从未见过的人民（世界无产阶级）”。

